VTT Technical Research Centre of Finland

Cyber Threat Actors for the Factory of the Future

Sailio, Mirko; Latvala, Outi-Marja; Szanto, Alexander

Published in:
Applied Sciences

DOI:
10.3390/app10124334

Published: 24/06/2020

Document Version
Publisher's final version

applied sciences

MDPI

Article

Cyber Threat Actors for the Factory of the Future

Mirko Sailio [1,*], Outi-Marja Latvala [1] and Alexander Szanto [2]

[1] VTT Technical Research Centre of Finland, 02044 Espoo, Finland; outi-marja.latvala@vtt.fi
[2] BIGS Brandenburgisches Institut für Gesellschaft und Sicherheit, 14482 Potsdam, Germany; alexander.szanto@bigs-potsdam.org
* Correspondence: mirko.sailio@vtt.fi; Tel.: +358401958601

Received: 30 April 2020; Accepted: 17 June 2020; Published: 24 June 2020

Abstract: The increasing degree of connectivity in factory of the future (FoF) environments, with systems that were never designed for a networked environment in terms of their technical security nature, is accompanied by a number of security risks that must be considered. This leads to the necessity of relying on risk assessment-based approaches to reach a sufficiently mature cyber security management level. However, the lack of common definitions of cyber threat actors (CTA) poses challenges in untested environments such as the FoF. This paper analyses policy papers and reports from expert organizations to identify common definitions of CTAs. A significant consensus exists only on two common CTAs, while other CTAs are often either ignored or overestimated in their importance. The identified motivations of CTAs are contrasted with the specific characteristics of FoF environments to determine the most likely CTAs targeting FoF environments. Special emphasis is given to corporate competitors, as FoF environments probably provide better opportunities than ever for industrial espionage if they are not sufficiently secured. In this context, the study aims to draw attention to the research gaps in this area.

Keywords: Factory of the Future (FoF), cyber threat actor; threat actors; corporate cyber espionage

1. Introduction

The managed information security strategy for an organization requires an approach based in risk analysis for efficient resource allocation and to document the due diligence required by law. Multiple common systems have been described for risk analysis. These approaches present the identification of cyber threat actors (CTAs) as a critical step in successfully designing a robust cyber defense for an organization.

Many information security organizations have defined classifications or lists of types of threat actors, threat agents or malicious actors. However, there is often no consensus on common definitions of the types of attackers, and often the reader must assume the perspective of the organization compiling such a list. Furthermore, organizations may tend to consider just one or only a few sources of information and thus to orientate their actions according to the corresponding scope of the classified threat elements of the respective report. This may result in overlooking a certain emphasis that the majority of security organizations have identified as a risk factor or over-emphasizing a CTA with minor effect in operating a real environment. Thus, there is a tendency to focus on quantitative factors (i.e., the number of occurrences of different threat actors mentioned in the respective reports) rather than qualitative factors (i.e., a competitive analysis).

This study has, therefore, systematically collected relevant literature on CTA from reports and strategy papers of national and expert organizations as well as industries, first to provide an overview and second to identify priorities and potentially ignored or underestimated risks. While industrial espionage is not a new phenomenon and has always been practiced by states and by competitors, the majority of expert literature shies away from discussing this threat actor in cyberspace or appears to

neglect them. At least the results of the assessment of the reports and strategy papers provide some indication of this.

Hence, this study aims to raise awareness of this subject, considering that the economic ecosystem is becoming increasingly interconnected, which is especially true for the factory of the future (FoF). FoF environments are promising great productivity gains and new possibilities for profitable business strategies. However, reality also shows that the implementation of these various conditions required by the FoF environment comes with serious cyber security challenges.

First, this paper studies the different CTA listings and identifies CTAs from multiple organization types from governmental institutions to cyber security industry experts. Second, the paper groups similar threat actors together to lessen the duplication of actors. Third, threat actors and their capabilities are then mapped to the characteristics of the FoF environment. Finally, the paper discusses the somewhat politely ignored role of competitors as threat actors and the concept of "hack back" as a controversially debated defense mechanism.

2. Analysis of Reports and Strategy Papers—Identifying Cyber Threat Actors

Threat actors are defined e.g., as an entity that is responsible for an incident that impacts or has potential to impact an organization's security [1]. This definition, however, is too vague to identify the real threats for an organization. This section will list threat actors identified by different authorities: national, cyber security expert organizations or industry leaders, to examine their kind and number of appearances. The nation, expert and industry organizations were selected given their importance in the field of cyber security, with the aim of obtaining a broad collection to identify similarities with documentation published in English to facilitate peer review.

CTAs identified by national authorities are collected by first analyzing reports published by relevant cyber security bureaus. Thereafter, the national cyber security strategies are considered. While national advice and official positions on threat actors may not be available in the languages known to the authors, broader level strategy papers typically are. We have also included the European Union Agency for Cybersecurity (ENISA) and the United Nations to this authority category even though they are international organizations. Their expertise and recommendations are in particular relevant for countries that do not have extensive and sophisticated technical (information technology (IT)) expertise, and they probably present an international consensus on the ideas. Since ENISA represents and is, as a cybersecurity umbrella organization, responsible for all European Union (EU) nation states; no national level analysis is made on EU countries, even though many would have been natural candidates for the list.

Other expert organizations and industry leaders have also published reports or communications describing the threat landscape of the internet. It is interesting to note that many reports avoided talking about threat actors, making them meaningless for our research. Some of the most notable were Rapid7, Symantec and OWASP (Open Web Application Security Project).

Table 1 shows the findings of the research on the reports and strategy papers. Identified CTAs are marked with an "X" and CTAs strongly indicated by the paper are marked with an "i".

Table 1. List of identified cyber threat actors (CTAs) based on international reports and strategy papers.

Strategy Papers	Nation-states	Cyber criminal	Hacktivist	Terrorist	Insider	Thrill Seeker	Hacker	Ind. Espionage	Corporation	Malicious Actor	Other *	Partner
National												
US NIST	X	X	X	X	X	X	i	X	-	-	-	X
ENISA	X	X	X	X	X	-	-	-	X	-	-	-

Canada CCCS	X	X	X	X	X	X	-	-	-	-	-	-
Japan NISC	X	X	-	i	-	-	-	-	-	X	-	-
Russia	X	X	-	X	-	-	-	-	-	-	-	-
India	X	X	-	X	-	-	-	i	-	-	-	-
Brazil	X	X	X	X	-	-	-	-	-	-	-	-
S. Africa	X	X	-	X	-	-	-	-	-	-	-	-
UN	X	X	-	X	-	-	-	i	-	-	-	-
China CAC	-	X	-	X	-	-	-	i	-	-	-	-
Expert												
SANS	X	X	X	-	X	-	-	-	-	-	-	X
CIS	X	X	X	X	X	-	-	-	-	-	-	-
CC	-	-	-	-	X	-	X	-	-	X	X	-
ISSA	X	X	-	-	X	-	-	-	-	-	-	-
ITU	X	-	-	X	X	-	-	-	-	i	-	-
Industry												
CrowdStrike	X	X	X	-	-	-	-	-	-	-	-	i
Verizon	X	X	X	-	X	-	-	-	-	-	-	X
IBM	X	X	X	-	X	-	X	-	X	X	-	-
FireEye	X	X	-	-	X	-	-	i	-	-	-	X
Symantec	-	X	-	-	-	-	-	-	-	i	-	-
Accenture	X	X	X	-	-	-	-	-	-	-	-	X
McAfee	X	X	-	-	-	-	-	-	-	-	-	i
Sum 22	19	20	10	12	11	2	3	5	2	5	1	7

2.1. National and International Cyber Security Organizations

2.1.1. US—National Institute for Standards and Technology (NIST)

The United States has multiple major agencies tasked in dealing with cyber security, the most notable perhaps being the National Institute for Standards and Technology (NIST). NIST has published a great number of reports and guidelines for cyber security. Their 800-82 guide for industrial control systems security perhaps the is best fitting [2]. The CTAs identified include national governments (nation-states), terrorists, industrial spies, organized crime groups (cyber criminal), hacktivists and hackers. It also refers to an additional source [3], which further includes thrill seekers and insiders as separate actors. Additionally, NIST has guidelines for conducting risk assessments, which identifies industrial espionage and partners for additional likely CTAs [4].

2.1.2. European Union (EU)—The European Union Agency for Cybersecurity (ENISA)

ENISA is an agency tasked in enhancing Europe's cyber security capabilities, mainly by conducting research and providing assistance to national cyber security actors in the EU. It published an annual threat landscape report until 2019 [5]. The identified threat actor categories have matured somewhat in the years the report has been published. The report also aims to identify actual incidents that have been published, and attributes those to the likeliest threat actor category. Their latest threat landscape report identifies cyber criminals, nation-states, hacktivists, cyber fighters, cyber terrorists and script kiddies (thrill seekers).

2.1.3. Canada—Canadian Centre for Cyber Security (CCCS)

The Canadian Centre for Cyber Security (CCCS) is the Canadian authority in cyber security. It has a cyber threat actor list [6] with expected motivations and typical sophistication included. It lists nation-states, cyber criminals, hacktivists, terrorist groups, thrill seekers and insiders as CTAs.

2.1.4. Japan—National Center of Incident Readiness and Strategy (NISC)

The National Center of Incident Readiness and Strategy (NISC), the Japanese government's cyber security authority has a public cybersecurity strategy [7]. It identifies the key threat actors for Japan being other nation-states and cybercrime. It also indicates that terrorist usage of the cyberspace needs to be monitored and understood.

2.1.5. United Nations (UN)

The United Nations (UN) has also been active in aiding to distribute cyber security awareness in its member countries. It is especially important for the countries that have less developed cyber security expertise. A recent report [8] identified cyber criminals, nation-states and terrorists as notable threat actors in the area. Industrial espionage was mentioned as well.

2.1.6. China—The Cyberspace Administration of China (CAC)

The Cyberspace Administration of China (CAC) publishes a national cyber security strategy since 2016 [9]. While the original document was not available in English, machine translation has enabled the authors to use text search for key terms. In addition to supporting meta-analysis documents [10], this enables crude level analysis on threat actor mentions with some level of confidence. Given the high importance of China in the area of cyber security, the strategy was included without access to the original text. CAC identifies cybercriminals, terrorists, and industrial espionage as a threat. Interestingly, China is the only state not listing nation-states as threat actors in cyberspace.

2.1.7. Russia

The Security Council of the Russian Federation has published the cyber security strategy of Russia [11]. It identifies nation-states, cyber criminals and terrorists as threat actors. The major focus of the strategy is on outside actors targeting social stability by using the cyberspace.

2.1.8. Brazil

Brazil has a complicated cyber security strategy spanning a multitude of different federal organizations [12]. It identifies state actors, cyber criminals, terrorist and hacktivists as threat actors.

2.1.9. South Africa

South Africa has published the National Cybersecurity Policy Framework since 2015 [13]. It identifies state actors, cyber criminals and terrorists as the main threat actors.

2.1.10. India

India is writing a new version of its National Cyber Security Strategy for 2020, with comments being presently requested [14]. The call for comments mentions state actors, cyber criminals and terrorism explicitly and implies high risk to business data (industrial espionage).

2.2. Expert Organizations

2.2.1. The SANS Institute (SANS)

The SANS Institute is an international cooperative research and education organization offering training and certification for information security professionals around the world. It is one of the biggest private organizations focusing on information security excellence.

SANS identifies cyber criminals, state sponsored threat actors, hacktivists, insiders (system administrators, end users, executives and managers) and partners as threat actors [15].

2.2.2. International Securities Services Association (ISSA)

The International Securities Services Association (ISSA) is an organization aiming to strengthen collaboration and mitigate risks within the global securities services industry. It publishes an annual cyber security risk management report for its members, including a threat agent analysis for the industry. The ISSA identifies nation-states, cyber criminals (organized crime), hacktivists, malicious insiders and unwitting insiders as threat agents [16].

2.2.3. International Telecommunication Union (ITU)

The International Telecommunication Union (ITU), a UN agency focusing on communications networks, identified nation-states, terrorist, disgruntled workers (insiders) and malicious intruders (malicious actors) as threat actors [17].

2.2.4. Centre for Internet Security (CIS)

The Centre for Internet Security (CIS) is a non-profit organization aimed to improve cyber security of private and public organizations. It identifies nation-states, cyber criminals, hacktivists, terrorists and insiders as primary threat actors [18].

2.2.5. Common Criteria for Information Technology Security Evaluation (CC)

The Common Criteria for Information Technology Security Evaluation (CC) is a technical basis for an international agreement aiming to ensure a common criteria for security properties of certified products. The CC describes examples of threat actors as hackers, malicious users, and non-malicious users. The report also describes computer processes and accidents as threat actors. Those are combined to the "other" column on Table 1 [19]. Its view of threat actors is unusual when compared to others, but its importance as a global standard merits its addition to the list.

2.3. Industry

2.3.1. Verizon

Verizon, an American multinational telecommunications company provides threat reporting to the public based on their customers' incidents. They report incidents originating from cashiers and system administrators (insider), supply chain partners, cyber criminals, nation-states and activists [20].

2.3.2. International Business Machines Corporation (IBM) X-Force Threat Intelligence Index

X-Force provides threat intelligence based on in-house research. It lists organized crime (cyber crime), nation-state, hacktivist and insider activities in their research [21].

2.3.3. CrowdStrike

CrowdStrike is an anti-virus provider, which publishes an annual report. The CrowdStrike Global Threat Report focuses on nation-states and cyber criminals. An additional focus is on supply chain compromises, pointing to the activities of partners as a possible threat actor [22].

2.3.4. Symantec

Symantec is a leading cyber security vendor, which has an annual report on cloud security [23]. It does not focus on identifying threat actors, but names cyber criminals and bad guys (malicious actors).

2.3.5. FireEye

FireEye is an information security vendor with strong threat intelligence abilities. It publishes a report on detected threat trends annually [24], containing results from their customers sensor systems. It creates great transparency in cyber security incidents. While it does not define threat

actors, its report lists state sponsored actors, cyber criminals and insiders and indicates partner or third-party actors. It also identifies espionage activity, likely in support of intellectual property or espionage end goals, indicating likely competitor activity.

2.3.6. Fortinet

Fortinet is a cyber security company boasting the largest device footprint in the industry. The feedback loop from these devices is reported quarterly in a threat landscape report [25]. It focuses on the results from their monitoring and identify cyber criminals and nation-state actors [26].

2.3.7. McAfee

McAfee is a leader in the cyber security and threat intelligence market. It publishes a quarterly threat report on detected cyber attacks and incidents [27]. It identifies nation-state actors, cyber criminals and supply chain partner attacks.

2.3.8. Accenture

Accenture is a global professional services company, which has expertise in a wide range of industries. It publishes an annual [28] report containing measurements based on its cyber defense system. It identifies cyber criminals, hacktivists, state-sponsored threat actors and compromised business partners as threat actors.

3. Classifying Cyber Threat Actors (CTAs)

CTAs are differentiated from others mainly by their internal motivation. Skill level, resources and other such attributes do not differentiate well between different CTAs (e.g., nation-states building their cyber offence program may be poorly resourced and lacking in skills while a hacktivist group with a rich patron may have almost limitless resources).

The previous section identified 13 different threat actors. Some of the threat actors have such similarities in their motivation, that they can be combined without losing the meaning of the category, see Figure 1. Hacktivists and terrorists have been grouped into ideologues, hackers have been merged with thrill seekers, industrial espionage and corporations have been combined to a competitor actor class. Some classes have been imported without change.

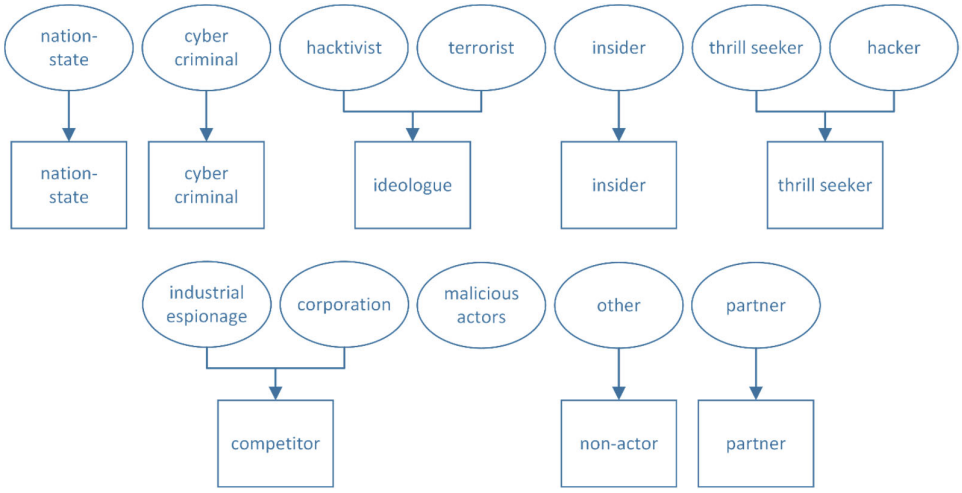

Figure 1. Identified threat actors combined into the eight categories discussed in this paper.

The malicious actor umbrella term does not have any differentiation power, so it is discarded as almost all threat actors can be considered malicious actors. Threats without an actor are placed in

a non-actor classification. Next, we describe the threat actor classes and the reasons for grouping in more detail.

3.1. Cyber Criminals

Cyber criminals infiltrate networks using any available and exploitable vulnerability. They have two objectives, to extract value (money, valuable items or valuable data) and to avoid legal consequences while doing it. One should keep in mind that a large portion of financial damage caused by cyber criminals is not direct, especially in industrial networks. Many schemes (e.g., ad fraud, loyalty program fraud) inflict mainly secondary (indirect) costs to their victim organization [29].

Some cyber crime groups seem to be state-sponsored and act for nation-state threat actors [30], so clear differentiation between cyber criminals and state actors may be impossible. Cyber criminals can also work for other third parties, even other cyber criminals, as a service (cyber crime as a service—CCaaS) [31].

Cyber criminal activity directed at organizations can be divided into three broad categories:

- Mass scams and automated hacking: these activities aim to monetize successful hacking using automated tools and mass scams to infect large amount of accounts and computers. They use crypto trojans for blackmailing and stealing easily sellable data (e.g., social security numbers, credit card numbers, passwords and bitcoins). They ssek to get value with minimum possible human effort. Special mention should be given to cryptojackers, who infect systems and then use those resources for mining crypto currencies. This gives the owners of the tools financial value without the knowledge of the owner of the system.

- Criminal infrastructure providers: these actors use automated hacking tools to infect as many systems as possible, and to consequently use those systems in a criminal infrastructure (e.g., botnets). They may then sell the utilization of this infrastructure to third parties for distributed denial of service (DDoS) attacks, spamming, bullet-proof hosting etc., or exploit it for their own campaigns. In these cases, an infected system may perform normally without any noticeable problems, until the system is placed on a public blacklist for malicious activity.

- Big game hunters: these cyber criminals use considerable effort to attack single high-value targets, especially high-value financial transaction systems (e.g., SWIFT hacks). These types of attack may apply custom designed malware, or conduct attacks through supply chain partners. The criminals invest considerable effort into studying the related technologies and network architectures, carefully engineering the attack and hiding their actions. High-value targets in an organization are also targeted by email and phone frauds, utilizing social engineering skills to enhance the wider attack [25,28].

Cyber criminals are very creative, they may both come up with novel attacks and resurface long-forgotten scams with a fresh perspective to make criminal gains. This is important to keep in mind, especially when discussing emerging technologies such as artificial intelligence (AI) or the ecosystem of the FoF.

Cyber criminals are the primary source of incidents in the wild [5]. It is important to note, however, that cyber crimes range widely from online tax fraud to romance scams [29]. Not all kinds of cyber crimes are relevant to the majority of organizations and an organization needs to apply proper risk-based cyber security management processes to identfy the relevant threats. Moreover, e.g., a tax fraud may not be directed at the organization but an insider committing such a crime could still impact it. Twenty of the 22 organisations identified cyber criminals as a CTA (Table 1).

3.2. Nation-State Actors

Nation-states can be considered as active threat actors in cyber security [5]. Their objectives are more varied than that of regular cyber criminals, typically aiming to gather intelligence or support

national interests (e.g., nuclear non-proliferation, financing, technology transfer and dissident control). The cyberspace toolset has enhanced the abilities that nation-states have already previously held, especially in espionage.

For the last 20 years, a lot of reporting has been published on cyber operations aimed at technology proliferation. In this, state actors have been tied to campaigns using industrial espionage to elevate the capabilities of domestic companies, typically tied to military technologies. China, for instance, has been especially effective bridging the technology gap using various methods.

Strategic sabotage is one of the techniques that nation-state actors use. Maybe the best known suspected nation-state cyber action was the Stuxnet incident [32]. In this incident centrifuges used by the Iranian nuclear program were sabotaged by infecting their air-gapped control systems with an advanced malware causing them to deteriorate. While the target was a state-run program, the attack path went through a commercial actor's control software.

Some states have been linked to cyber activities which indicate usage of cyber operations to enable other state activity limited by international sanctions. The SWIFT banking system attacks have been linked to nation-states using it as a way to finance their operations under strict economic sanctions [33]. These operations can be thought of as infrastructure enabling other activities. In smaller scale, nation-state actors using cyber operations for their aims may also need botnet infrastructure to maintain ability to use and mask cyber operations.

Ukrainian and Georgian critical infrastructures have both been subject to cyber operations seeming to originate from Russia. These cyber operations have similar aims as conventional military attacks on infrastructure, but without the need of a full blown war, with international condemnation and sanctions following. Cyber war operations however can be hard to attribute to specific actors, and there is always plausible deniability [34]. Even when attribution is reliable, there are a lot of legal gray areas to hide [35].

Nation-states target not only other nations, but also organizations (e.g., companies and non-governmental organizations (NGOs)), and they also practice mass surveillance of individuals. The stated aims are typically counterterrorism work and internal security. One more recent aspect for state actors is political campaign interference [36].

There are at least two major paths to national cyber operation capability. Some nations use well-funded intelligence agencies, while others use cyber criminal organizations. Such state sponsored groups are typically easier to identify, but have had a higher degree of deniability by the state [24].

It should be noted that, for most organizations, propaganda operations by nation-states (e.g., fake news, troll farms, social media manipulations) are not a valid cyber threat. Moreover, operating in certain nations may force the organization to adhere to that country's cyber laws (e.g., national firewalls, domain name system-DNS blacklisting, legal backdoors to systems or mass surveillance of people). These are also out of the scope of cyber security policies and our paper.

Nation-states activities present a large part of documented cyber incidents in the wild. It represents the second largest source of measured cyber incidents [5]. In the analysis 19 of the 22 organizations identified nation-state actors as a CTA (Table 1).

3.3. Ideologues (Hacktivist and Terrorist)

This paper combines the hacktivists and terrorists under the same threat actor category due to obvious similarities in operational aims. Hacktivists are activists who are ready to disobey computer security laws in their activity to advance their cause. Terrorists are groups of people aiming to cause terror to advance their cause. While the results of their activity are very different, both actors are ideologically motivated.

Additionally, the use of a terrorist label is problematic, as the label it used subjectively by nation-states and organizations. Terrorists often seem to be freedom fighters on the other side of a conflict. The government of Iran might classify the Stuxnet incident as an act of cyber terrorism, while the West typically considers it a nation-state activity [37]. The definition of cyber terrorism has become more indiscriminate for many organizations and some define any activity by a terrorist group in the internet (e.g., recruitment, money laundering, propaganda) as cyber terrorism. For example, the

Japanese Cyber Strategy [7] refers to the need to monitor terrorist organizations that use cyberspace for demonstrations, recruiting citizens and raising funds for violent extremism.

Those following an ideology and willing to perform terrorist activities by using computers are defined to belong to the same category as activists in this paper.

While an amount of activity by these actors is present, it is much smaller, than that of cyber criminals and nation-state actors. In addition, activists are typically a known threat to organizations they target. It is interesting to note, that while 12 of 22 identify terrorist threat actors, the authors were not able to find a clear cyber terror event documented. However, just 10 of the 22 organizations identify hacktivists as a CTA (Table 1), and about 5% of reported cyber security events can be classified as hacktivist activity in 2017 [38].

3.4. Thrill Seeker

A thrill seeker is a person, who attacks computer systems merely to prove himself, in order to learn or experiment. In the 1980s and early 1990s they were just known under the broader term "hacker", or white-hat hacker. While thrill seekers are not interested in damaging systems, they are interested in figuring out how things work and may cause surprising problems to systems and products.

While thrill seekers may cause problems, a well-organized vulnerability bounty program can turn these actors into cheap testing engineers. Especially vulnerability researchers are active in this area and it can be a great tool for enhancing one's product robustness and a good way to demonstrate to the community that security is taken seriously. However, an organization's inaction and inability to communicate vulnerabilities has e.g., triggered such actors to publish their findings, see the rather recent disclosures of Netflix [39] and Zoom [40] vulnerabilities as an example. Only 4 of the 22 organizations identified thrill seekers as a CTA (Table 1).

Script kiddies also apply tools developed by other actors to test and study cyber security techniques. While professionally managed systems should not be corruptible to script kiddies, there is always some risk and thus it is important to consider these actors. They can in fact be used as a minimum cyber defense capability meter stick: Unless you detect a constant background noise of network traffic caused by unskilled probing and automated attack tools, your organization's detection capability is probably not sufficient.

3.5. Insider

Insider threat actors can be separated in two categories: a mercenary insider and a disgruntled employee. Mercenary insider sells access to a network to other actors, while the disgruntled employee feels that they have been mistreated and causes problems to the organization in terms of retaliation. This often happens after they have been dismissed from their jobs. It is worth noting that insider threats include unintentional misuse. However, an unintended misuse does not have definable motivations and thus is left out of insider CTA activities.

It is challenging to prevent insider activity as people require access to business secrets and systems in order to fulfill their tasks. Insiders are typically detected following their successful activity by efficient logging and analysis. Finally, insiders may be exploited by other threat actors (e.g., cyber criminals), but in such a case they are considered to be threat vectors rather than threat actors, see Figure 2 below. In the analysis 11 of the 22 organizations identified insiders as a CTA (Table 1).

3.6. Competitor

In 1992, Frederick B. Cohen first described economic rivals/competitors as threat actors for the National Information Infrastructure (NII) and highlighted the technical capabilities and expertise of some IT-companies that have the means to disrupt the NII or gather economic intelligence [41]. The shortcut of industrial espionage, however, has always been an effective means of gaining access to blueprints, recipes and other company secrets that should be well guarded in order to protect the often considerable investments that many companies make to develop intellectual property. The list

of spectacular cases is long and is often garnished with cases that run along the boundaries in the grey area of legality. When Oracle had to admit that, it had hired a detective agency to investigate connections between Microsoft and advocacy groups, Oracle's CEO L. J. Ellison justified the years-long espionage with a public service and a "civic duty" [42].

In the mid-2000s, Deloitte even employed an entire team consisting of accountants, former veterans and intelligence officers who conducted covert operations for the company to obtain as much information as possible about competitors and were exploring how to attract future clients with information about their competitors [43]. The team was composed of information gatherers and analysts responsible for spying on other major consulting firms about their products and business models. In this context, the unit became active as BearingPoint—a major consulting firm at that time that, unknown to the public, was financially in trouble but had many federal contracts that were lucrative for competitors—and partners from around the world gathered for a meeting in Orlando, Florida [44]. Eventually, Deloitte acquired the federal business division of BearingPoint, and the information obtained in dubious ways may have played a certain role.

These examples illustrate that economic rivals have long been a threat to a business and not just since the technical capabilities the internet offers to spy and hide. Thus, it is all the more surprising that only 7 organizations have a competitor listed as notable threat actor (industrial espionage or corporation on Table 1). This is quite low when considering the likely advantages of adopting offensive cyber operations' activities in hard fought markets. Offensive cyber operations open possibilities for business intelligence and active operations to foil the launch of key systems.

Business intelligence and knowledge acquirement are the clearest benefits available from offensive cyber operations. This information can be used for e.g., timing marketing campaigns and product launches to ensure the best possible impact. Businesses can also benefit hugely from knowing the trade secrets of a competitor, enabling better targeting of products of their own to the market.

3.6.1. Competitive Intelligence

Competitive intelligence, sometimes referred to as business or corporate intelligence was coined by the American strategy professor Michael Porter [45]. Porter is considered the father of competitive analysis, a concept he described in 1980 in his book "Competitive Strategy", which in digital interpretation often conceals a corporate espionage strategy [45].

While competitive intelligence in its original sense meant collecting and analyzing all publicly available information about suppliers, customers, media coverage and patent databases of competitors, the methods used by some companies nowadays are partly in a grey area or already illegal.

To contextualize these developments, it is necessary to consider the circumstances and trends in politics, the economy as well as society in the last few decades and to understand the related rational of the economy. The boundaries for defining acceptable ethical practice are increasingly blurred, especially as surveillance technologies and espionage tools have become so accessible. In an environment that is paradoxically marked by mistrust and increasing dependency, the power of game theory becomes evident. Actions and decisions of competing players will affect the outcome of the respective market player and, in the theoretical framework, produce optimal decision-making by considering the behavior of competitors and acting accordingly to adopt the best approach for them individually [46].

3.6.2. Corporate Sabotage

In tight competitive situations, where there are not many competitors, corporate sabotage may be a seductive option. The aim is typically to damage the reputation of a key competitor. This can be achieved e.g., by hiring the infrastructure for a DDoS attack from criminals to disable a website or system, or by cyber attacks that aim to extract data that can harm the company in question for example by leaking sensitive or humiliating data to the public in various ways.

While the majority of cyber operations are now considered illegal, there are still some gray area activities, which companies can take, without breaking any laws (see Figure 2 for an illustration of this idea). The wide gray area in the legal space in most jurisdictions is likely due to an insufficient number of legal cases refining the boundaries into case law.

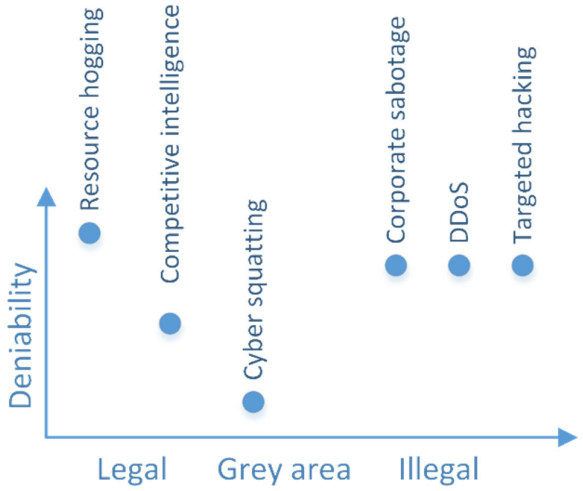

Figure 2. Illustrating the legality and deniability of different competitor actions (not to any scale).

A competitor can also be a non-business organization such as a political campaign. For example, in the 2016 U.S. Presidential Elections cyber operations played a part in the outcome of the elections [36]. Additionally, some legal tactics are publicly used (e.g., cybersquatting) which might not be ethical or even legal in some nations [47].

This complex of themes is addressed by the equivalent retaliation theory known as a strategy from game theory. It aims to define hostile actions between actors based on their previous relation history [48]. For example, if two parties used to have a cooperative relationship and part A has at some point acted harmfully to part B, part B will wait for an opportunity to harm part A in the same way that it was harmed. In political parties, this is considered a lack of trust between e.g., the party and the party member, which could be caused by a party policy that harms the party member [49]. The party member could then act in the same way on a given occasion to protect himself and regain what has been lost. Similarly, parallels exist between competing corporations, in the sense that in a market businesses also go beyond the legal barriers and the harmed business may also go beyond the threshold to cause the same damage.

The majority of consequences for organizations considering offensive cyber operations derive from the eventuality of being caught. Sadly, nation-states have already demonstrated the efficiency of plausible deniability in the internet [34]. Data pointing to competitors may be rare for this reason.

Overall competitors may be underestimated in typical threat agent identification. Further discussion on competitor activity is in the discussion section of the paper.

3.7. Partner

Partners enjoy the trust of the decision makers in the organization. They can be sub-contractors, vendors, clients, auditors, suppliers, authorities etc. This trust can be abused by using it as a lever in social engineering. Problems may also arise from the network access a partner, especially a vendor, has to an otherwise secure network.

Only few of the authorities identified partners as a threat actor. While it is unlikely that a partner acts with malice, it is much more likely, that the trust placed in a partner can be exploited by malicious third parties or the partner unintentionally compromises the cyber security of a system [27,28].

Additionally, using cloud computing gives rise to new partner threats. Cloud infrastructure providers need to establish a trusted relationship, as their systems security is often a black box to their customers. Some have dedicated hardware making third-party attacks harder but losing much of the scalability benefits of cloud infrastructure usage. Only 7 of 22 organizations identified partners as a CTA (Table 1).

3.8. Non-Actor

Some threats are not based on activities of a threat actor but are caused by exceptional circumstance or "acts of god". Such threats can be a source of serious problems (e.g., natural disasters, war, pandemics), and while this paper mentions them to provide a comprehensive overview, they are out of scope of the paper.

3.9. Hierarchy of Threat Actors

In Figure 3 we present the idea of a threat actor hierarchy. The CTAs higher up on the hierarchy can take advantage of those below them [28]. This can be done by offensive cyber operations targeting the other threat actors or by other means (e.g., coercion, tricking or bribing). Therefore, the top threat actors have more attack paths they can take and are able to better obfuscate their involvement.

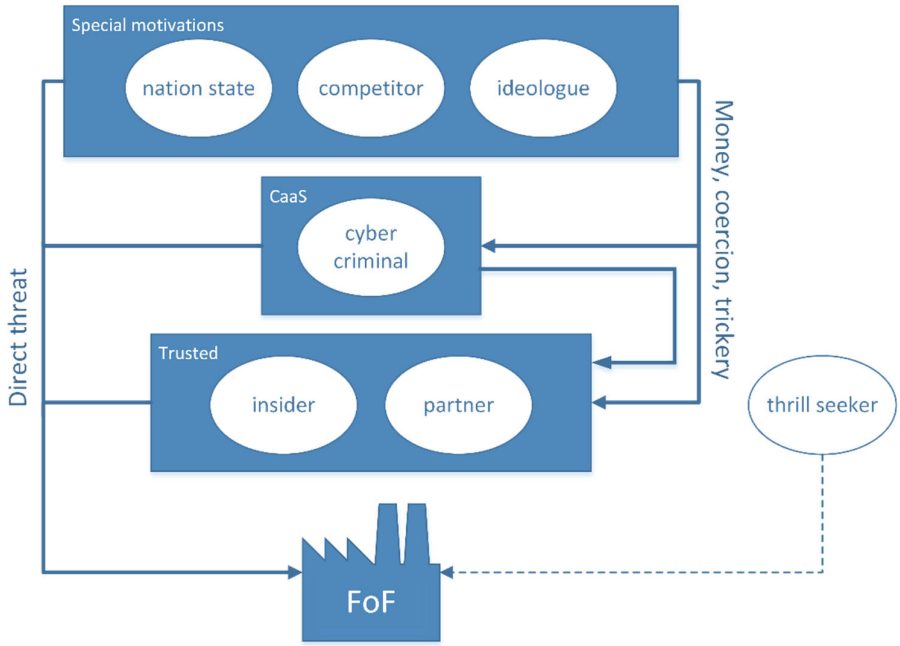

Figure 3. The threat hierarchy. Cyber threat actors (CTAs) at the top of the hierarchy use other actors as threat vectors. Criminals can be hired (cyber crime as a service (CCaaS)), and trusted actors can be bribed, coerced or deceived. Thrill seekers pose only a minor threat to the factory of the future (FoF) environment.

The threat actors on the lowest level, insiders and partners, are grouped together because the FoF needs to place a great deal of trust in these actors in order to function. This position also makes them a tempting target to all the other CTAs higher in this hierarchy. Insiders and partners may be bribed or coerced into working knowingly against the interests of the target, or they may be hacked and deceived into becoming a threat. The trusted position also enables them to inflict direct damage to the FoF for their own reasons, or by accident.

The thrill seeker CTA is placed outside the hierarchy, because they are only a minor direct threat to a properly set up FoF. Moreover, since a thrill seeker's motivation is internal (learning, fun) and there is typically no point for the other CTAs to use them.

The cyber criminals are a clear, direct threat to the FoF. Because some of them offer "cyber crime-as-a-service" to other actors, they are placed in a medium position in this hierarchy.

Nation-states, competitors and ideologues are grouped together at the top of the hierarchy: they can use the other CTAs to their advantage but no other CTA can use them, because these CTAs are mostly internally motivated. They may also want to specifically hide their involvement, and actually prefer indirect attack routes through, e.g., criminals or insiders. This gives them additional layer of obfuscation and plausible deniability, even when their activity is discovered.

4. Threat Actor Landscape for the Factory of the Future (FoF)

This section discusses the different threat actors in connection to the FoF operating space. As there is no strict definition of a FoF, its cyber security strengths and weaknesses are also still unknown. In this section we find the most important characteristics of a FoF from cyber security point of view and compare the threat actor landscape to those characteristics.

4.1. Definition of the FoF

A high degree of networking of the manufacturing landscape, data processing in real time across systems and the associated supply chains characterize advanced industrial landscapes today. The generic term Industry 4.0 encompasses all these developments as a concept for the networking of the industrial landscape. The term was coined in Germany in the early 2010s and since then has prompted many technical/scientific publications worldwide [50]. The integration of existing technologies and tools such as embedded systems, sensors, and other industrial hardware to enable real-time data processing reflects the Industry 4.0 ecosystem. Within this ecosystem, the CyberFactory No. 1 project (see: https://www.cyberfactory-1.org/en/home/) aims to design, develop, integrate and demonstrate a number of key capabilities to enhance the optimization and resilience of the FoF.

Additive manufacturing, autonomous machines, collaborative robotics, machine learning, augmented reality, big data analytics and many more technologies and digital methods/processes are connected to the environment of the FoF. A white paper from the World Economic Forum [51] found that factories that were able to push beyond just piloting these new technologies were those that embraced three key elements at scale: connectivity, intelligence and flexible automation. These elements bring with them cyber security challenges that have not been much discussed.

The feature of high connectivity is especially interesting from a cyber security point of view. A FoF may be permanently connected to the internet at many points, cloud manufacturing (CMfg), industrial internet-of-things (IIoT) so that meshed networks may be utilized, and IT and operational technology (OT) systems may be interlocked. These connections create new opportunities for traditional attack patterns, and certainly new attack vectors to target the FoF.

While widespread connectivity may include connections to other organizations, it is important to make a distinction in order to better understand different cyber threats for each aspect. To this aim, we separate network connectivity and collaboration from each other [52].

One can look at the intelligence aspect of a FoF from two perspectives: On the one hand, machine learning or other AI techniques enable the use of autonomous robots or machines that can learn and work beside humans on the factory shop floor. On the other hand, big data decision making can help optimize processes along the whole value chain, from engineering to customer service.

Flexible automation is enabled by the connectivity and intelligence of a FoF. It allows quick and aligned reactions to unusual situations, being able to customize products according to customer needs as well as reducing waste in time and materials. New ways to manufacture products in a flexible manner include, e.g., additive manufacturing (3D printing) and cloud manufacturing.

This paper will use the network connectivity, collaboration, intelligence and flexible automation as the defining features of the FoF. While they are often dependent on each other (e.g., collaboration and flexible automation require a high degree of connectivity) they give better base to consider different threats to the system and to identify the most meaningful cyber threats and CTAs affecting the FoF environment. The authors do not hold the position that this division includes all aspects of

all FoF environments or that all FoF environments have all of the listed aspects. The division is used more as a tool to identify the main aspects of FoF.

4.2. Threat Actors for the FoF

Collaboration, network connectivity, intelligence and flexible automation provide new possibilities for threat actors as well. In this section, we discuss how the identified eight threat actor classes can affect these properties. The connections are summarized in Figure 4.

4.2.1. Collaboration

While good collaboration can be used to enhance productiveness and even cyber security, opening up systems for a larger number of participants also increases inherent insecurity that is present in any complex system. The need for better tools enabling secure operation while collaborating will continue to grow. CTAs best capable of taking advantage of these vulnerabilities are well funded and motivated. Nation-state actors and cyber criminals are the most likely to thrive in such an environment.

A collaborative environment also includes network and resource access for the trusted partners. This enhances the risk of attacks via these partners' access channels. CTAs are well motivated and financed to take advantage of identified vulnerabilities. Nation-state actors are the most likely to abuse such connections. While partner CTAs are not expected to be actively attacking the subject organization's systems, their connections may be used for the attack or their insiders may be bribed or coerced to provide access.

4.2.2. Network Connectivity

The network connectivity of the FoF systems brings with it an increased attack surface. While network cyber defense is not a new subject, the requirement for complex interconnections between resources using multiple wireless and wired connections make the environment very challenging. Figure 4 shows connections of threats.

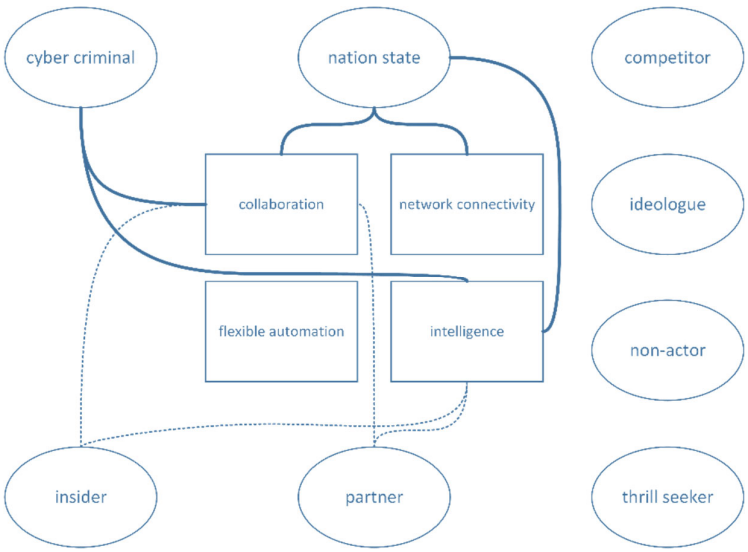

Figure 4. How the threat actors and features of a FoF are connected. Direct threats are marked with solid lines and threat vector access with dashed lines.

The network connectivity of the FoF systems brings with it an increased attack surface. While network cyber defense is not a new subject, the requirement for complex interconnections between resources using multiple wireless and wired connections make the environment very challenging.

Continuous access to the internet is required to implement the efficient usage of cloud resources. The challenges involved in securing internet-of-things (IoT) devices must be taken into account when planning and operating such systems. Such a challenging environment provides a wide attack surface and will require a mature cyber security management strategy as well as better tools in order to reduce the likelihood of cyber incidents. While all CTAs benefit from an environment that is harder to defend, the most likely CTAs to benefit from the additional connections are nation-state actors, who have the resources to target any component in the system. Furthermore, attackers only have to be successful once, whereas systems and their defenders have to constantly face new security challenges. Thus, the defending side is always under pressure and disadvantaged in this context.

4.2.3. Intelligence

Intelligence of a FoF is based mainly on machine-learning techniques that enable machine autonomy and usage of big data for decision making and optimization of operations. Adversarial machine learning techniques enable a highly skilled attacker to teach the machine-learning algorithm to manipulate the system in surprising ways. Additional risks from big data usage are mainly already covered in network connectivity, as the risks are similar. Big data applications also centralize the data into a big and juicy target for potential attackers. Cloud operators are skilled in normal cyber security management, so low resource attacks are unlikely to succeed.

Therefore, actors benefitting from the intelligence aspect are patient and highly skilled attackers—primarily state actors and cyber criminals targeting high-value targets. Insider and partner CTAs may benefit from a centralized data source architecture requiring a single system to gather all required material. Access to the data lake must be well designed and managed to prevent abuse adopting compartmentalization and the principle of least privilege where possible. Intelligence aspects may also lead to new non-actor based threats (e.g., unstable learning).

4.2.4. Flexible Automation

The flexible automation aspect of a FoF does not bring any clear advantages for the identified threat actors. Because the flexibility is predominantly enabled through the connectivity and intelligence aspects of the FoF, the discussion above holds here too. Additive manufacturing is an emerging manufacturing technique, but it is very physical; a CTA would again need to use the network connectivity aspect to affect it. In conclusion, while cyber criminals and nation-states are likely to find ways to abuse the system in a novel way, the same threats are present in current manufacturing systems already (e.g., vendor backdoor breach, update corruption).

4.2.5. Assessment of Threat Actors for the FoF

Prediction is very difficult, especially concerning the FoF. However, by combining the special characteristics that FoF environments have, we can make estimates on the most probable threat actors affecting FoF environments.

FoF environments are likely to be a composed of shop floor industrial networks combined to the industrial internet and cloud resources. This poses challenges to information security management.

Industrial networks have parts that have highly specialized equipment requiring highly specialized know-how. However, when access is achieved, the networks are often easy to disrupt due to high-availability requirements preventing the usage of security-enhancing techniques (e.g., security monitoring, encryption).

The networking aspect of the FoF environment is typically operated under a more robust security management strategy. The environment, however, is typical of many CTAs, meaning that while attacks against any secure cloud provider require expertise, the more skilled attackers may already have tools available. New partners and de facto insiders who manage the infrastructure used by FoF uses will considerably increase the attack surface. The new tools and techniques require vigilant information security management for a secure application. This combined with the soft foundation of industrial networks, makes the systems very attractive to many CTAs.

In Table 2 we present our assessment of how the observed threats listed in ENISA's 2019 report [5] relate to threat actors and the four aforementioned aspects of a FoF: network connectivity, collaboration, flexible automation and intelligence. Threat actors are given the weight of "1" if the CTA is a primary threat and "0.5" if they are considered a secondary threat by the report. This enables an estimation of how widely different CTAs take advantage of the most common threat types. The table shows an estimate of the most likely feature of the FoF to be affected by this kind of threat and is ordered so that the most often detected threat is on the top. Note, that partner and thrill seeker CTAs were not present in the report [5].

Table 2. Mapping 2018 observed threats [5] to CTAs.

Top threats 2018	Cyber criminals	Nation-states	Competitors	Ideologues	Insiders	Affected FoF aspect
Malware	1	1	1	0.5	-	Network Connectivity
Web Based Attacks	1	1	1	1	-	Network Connectivity
Web Application attacks	1	1	1	1	-	Network Connectivity
Denial of Service attacks	1	0.5	0.5	1	-	Network Connectivity
Botnets	1	1	1	1	-	Network Connectivity
Phishing	1	1	1	1	1	Network Connectivity Collaboration
Spam	0.5	0.5	0.5	-	1	Collaboration
Ransomware	1	1	1	-	0.5	All
Insider Threat	1	0.5	1	0.5	-	All
Physical Manipulation/ Damage/Theft/Loss	1	1	1	0.5	1	Flexible automation
Exploit Kits	1	1	1	-	-	Collaboration Network Connectivity
Data Breach	1	1	1	1	1	Network Connectivity
Identity theft	1	1	1	1	1	Collaboration
Information leakage	1	1	1	0.5	0.5	All
Cyber espionage	-	0.5	0.5	-	0.5	Collaboration Network Connectivity Flexible automation
Total	13.5	13	13.5	9	6.5	-

The table shows threat actors in all categories being able to mount offense against FoF environments using existing techniques. Especially high scores are gained by cyber criminals, nation-state actors and competitors. In this analysis competitors threat technique capabilities match those of nation states and cyber criminals.

4.2.6. Analysis of different CTAs for the FoF environment

Cyber criminals are the most prolific threat actors in the general cyber security space. They target a wide range of industries and have a cornucopia of monetization techniques to take advantage of. FoF systems will likely be targeted by cyber criminals as long as there is a profit to be made and the stakes remain low. They are likely to adopt traditional methods in a creative way into the new environment, as they have before, and are most likely the primary source of incidents in FoF environments. This is also mirrored in the current threat reporting as seen in Table 2.

Nation-state actors are interested in strategic data, espionage, and economic espionage, capability to control critical infrastructures and disrupt critical production chains. They are also interested in the capability to disrupt decision making and to interfere in competing state leadership selection. Many of these aims may be achieved by targeting FoF environments. Nation-state actors have the high skills required for breaching FoF environments. As the nation-state actors have no need to make a profit, they are most likely to use third parties as a threat vector for offensive cyber

operations. Nation-state actors are a likely CTA for FoF operator as seen in Table 2 and are likely to stay that way in the future.

Competitors are typically those with the most to gain from offensive cyber operations. They are typically thought to be held back by ethics or fear of reputational damage, but data on the real usage of cyber operations against competitors is lacking. They are a CTA that is likely to be underestimated by authorities. Competitors are likely to have deep specialist knowledge of operating similar specialist systems required for delicate manipulation of industrial systems. They are likely the source of the more intelligent threats targeting FoF environments, as they have industry knowhow, contacts and understanding. This is especially true in business areas where there is lack of competition or with state controlled/backed businesses that work in areas of military or intelligence importance (e.g., aerospace, communications). A state-backed competitor may also lack any real choice in initiating offensive cyber operations and can have immunity to any real consequences even when getting caught. Current threat trends (Table 2) indicate that competitors are an important CTA for FoF environments and will remain so in the future.

While partners are not a likely source of cyber incidents, they are a likely attack vector used by other CTAs. They should be considered as great of a threat actor as insiders, and can easily be bribed, coerced, tricked or even compelled to collaborate by law. The high connectivity and collaboration of FoF environments make partners an even more important threat actor than typical environments.

Insiders need also to be kept in mind as a threat actor. They too can be tricked bribed or coerced to giving access for other CTAs. Any insider access is a source of wider problems in FoF environments when using centralized data collection systems and collaboration tools, so the result of a compromise by an insider is likely more devastating in such an environment. The low score in Table 2 for insiders should not be considered to lessen the importance of insiders as a CTA as they likely do not need to contend with the cyber security systems protecting the FoF environment.

Ideologues are a less likely threat actor for a typical FoF environment. A majority of hacktivist actions are website defacement not included in typical FoF environment. Terrorist activity against most FoF operators (e.g., manufacturing) remains unlikely. However, the current trends indicate ideologues being active in threat areas that can affect FoF environments (Table 2). The FoF operator should consider if their organization is an interesting target for an ideologue.

Thrill seekers are also likely not a major threat actor for well-managed FoF environments. While historically hackers have been a cause of massive well known cyber security incidents, they are now dwarfed by the constant activity of nation-state and cybercrime CTAs. Thrill seekers are not likely to expend the effort to breaching the defenses required for a FoF environment. They will continue to find vulnerabilities on subsystems of the FoF environment causing problems for the unprepared and presenting opportunities for those who are well prepared.

5. Discussion

This paper presented the threat actors that different expert organizations identified. Table 1 shows the number of mentions in different organization's threat agent identification. The number indicates how many organizations out of the 22 identified the threat actor in their documentation. The commercial interest of private IT and cyber security vendors should certainly not be ignored, as they frequently refer directly or indirectly to their in-house solutions, such as cyber security based on artificial intelligence (AI) or cyber insurance. Consequently, studies authored by IT and cyber security organizations should be handled with some caution, as these organizations have a commercial interest and allow a somewhat biased view of the scope, usually based on anonymous customer data. Nevertheless, certain tendencies are discernible, which can be deduced from the comparison with public institutions and government agencies.

The organizations mapped by our report analysis had big differences in identifying the CTAs. While the top threat by incident numbers was clearly cyber crime, not all of the expert organizations identified them as a CTA. Nation-state actors were identified by the majority (19 of 22). However, the greatest mismatch in the public incident data and threat actor identification was with terrorist actors. Of the 22 expert organizations 12 identified cyber terrorists as a significant threat actor, while still no

clear terrorist cyber incidents have been documented. In our data, only 7 organizations identified competitors and only 6 identified partner organizations as an important CTA.

In this context, it should be noted that companies that have become victims of industrial espionage tend not to go public. The reasons for this are very different. Damage to reputation certainly plays a significant role, since depending on the magnitude of the incident, the industry and the size of the company concerned, the damage caused by public disclosure is perceived by many companies as more significant. Furthermore, the perpetrators are not always identified, nor is the extent of the incident. Sometimes companies do not even know what kind of information were actually extracted. The estimated number of undetected cases is likely to be high.

Nevertheless, cooperation between national authorities on cyber security and the fight against cybercrime has led to increased trust and transparency in dealing with incidents, as the problem is systemic rather than selective and affects everyone almost equally. On the other hand, companies in the critical infrastructure sector, for example, are obliged to report incidents (see also the EU Directive on Security of Network and Information Systems (the NIS Directive)) as well as companies in the EU that are affected by a data breach (see also the General Data Protection Regulation (GDPR)) and are liable to prosecution if they conceal incidents. Overall, the industry is in a state of constant change.

5.1. Competitors—The Politely Ignored Cyber Threat Actors

The technological development of the last two decades has made industrial espionage easier, cheaper and more effective and has further diminished the inhibition threshold due to the reduced pressure of law enforcement. At the same time, concern about reputational damage results in victims not always making such incidents public.

The accusation of industrial espionage also concerns a company that has experienced a rapid rise in the field of telecommunications equipment and is nowadays a global leader in many areas of telecommunications technology. The fast and global rise of Huawei is repeatedly accompanied by lawsuits in which competitors sue the Chinese company for various offences related to the theft of trade secrets. In early 2020, the U.S. Department of Justice accused in a federal indictment the Chinese telecommunications equipment supplier, who has been in the headlines for months, of stealing trade secrets and racketeering [53]. Huawei is accused among other things of allegedly misappropriating source codes from competitor's products to illicitly acquire technological know-how [54].

This accusation, however, affects not only individual companies, but entire nations. The suspicion that countries use some of their companies to carry out espionage in a networked world to gain critical knowledge about technology and achieve strategic goals has been raised for many years [55]. China, in particular, is repeatedly confronted with such allegations, as many companies are state-owned or closely linked to the Communist Party. Attempts to gain access to key technologies through the acquisition of companies are also viewed with suspicion. The growing pace of globalization and the associated merger and acquisition (M and A) activities of larger corporations, may lead target countries to consider the takeover as a threat to national security and possibly impose restrictions, as companies could be exploited as espionage instruments by foreign direct investment [56].

That this mistrust between states is not a recent phenomenon, as cyber espionage appears to be more of a concomitant of connectivity than an exception, is shown in a case from 2011. In May 2011, Huawei acquired the almost insolvent US start-up 3Leaf for a low single-digit million sum [57]. 3Leaf developed a technology for dynamically scalable supercomputers. While Huawei had already acquired the company with all its intellectual property and some employees, the Committee on Foreign Investment in the United States (CFIUS), which is an overarching US government committee to control foreign investment, intervened. Eventually, Huawei had to withdraw from the purchase after a divestiture mandate of the CFIUS, in which an appeal against the decision would be under final authority of the US president. However, political and military interests often mix with economic considerations so that decisions lack transparency, and it is often not discernible whether they are guided by genuine national security concerns [58].

These discussed cases show that the range of industrial espionage is fairly wide, both in terms of actors, their means and intentions. While business secrets in the analogue world were also threatened by disgruntled employees who wanted to harm the company, or by insiders looking for a quick buck by providing sensitive information to competitors, new, supposedly easier ways to obtain trade secrets have emerged in the digital market in a legal grey area.

Although competition cannot always be seen as a zero-sum game in which the gain of one party is equivalent to the loss of another, this is usually the understanding in which a battle for resources, customers and strategic goals is waged. At the same time, boundaries between state and corporate espionage are vanishing [59].

Thus, it will not become easier to distinguish economic from political and/or military intentions, and thus an increasingly globalized economy becomes in part more nationalistic and mistrustful. It is a paradox that the digitization of the world was actually intended to overcome this. The question is how long two seemingly irreconcilable tendencies can exist in one market.

The real world measurement of competitor activities is a hard problem. Usage of subcontractors, plausible deniability and other techniques can hide the final beneficiary of a cyber attack. The situation is confused even further by some states activities to use state cyber offensive abilities to benefit key companies. This section discussed industrial espionage more broadly and pointed out that the actual numbers of cyber espionage targeting competitors is likely much higher than assumed.

5.2. Hack Back Operations as Part of the Solution or the Problem?

As a means of protecting against the rising tide of cyber attacks, there has been increasing debates about so called "hack back" or "active defense" options. When U.S. representatives first introduced the Active Cyber Defense Certainty Act (ACDC) in 2017, U.S. Members of Congress wanted to allow companies to chase the attackers and take a more aggressive cyber defense approach [60]. This legislative initiative is still preoccupying the U.S. Congress and is the subject of controversial debates in the cyber security community as well as among private companies and various security authorities. The debate focuses on three relevant aspects: attribution, the implications and scope of hack back operations and the status of the state's monopoly on the use of force.

Attributing an attack and identifying the responsible parties hiding behind an operation is not that easy in cyberspace. First of all, it depends on whether you need watertight evidence that allows a prosecution in court, or whether strong evidence from different sources is sufficient if the political stakes are sufficiently high. Since the Computer Fraud and Abuse Act of the U.S. Congress was enacted in 1986, the legal situation for companies and individuals has in fact been unambiguous. No one is by law permitted to access a computer knowingly and without permission. The ACDC Act would thus create a judicial area that legalizes hack back and thus partly overtakes the 1986 act. Thus, the target of a hack back operation would depend on the skills of the company IT department or the dedicated cyber security company and would be limited to the accessible, mostly technical, attribution resources. False-flag operations that aim to create a false trail and hide behind many nodes can cause innocent parties to be targeted by the defenders and provoke a retaliatory action. Yet companies overestimate their attribution capabilities and present allegedly reliable evidence that is not [61].

The question of proper attribution is, thus, also related to the countermeasures and the implications they might have, depending on who is actually masterminding an attack. Does this create more security or more insecurity, and what happens when companies hack nations and if they in turn retaliate? According to this understanding, the cyber world is perceived as an anarchic environment as there is no uniform and comprehensive legal framework restricting everyone connected to this world from doing whatever he/she wants. In that case, cyberspace is more or less an international relations arena that different powers compete over for regional hegemony (market hegemony). In that cases hack backs are not illegal, but not in any way legalized. Hack back is described as a Wild West strategy or a vigilante justice [61] that should raise concerns, if self-defense is something that should be perceived as something acceptable. Should the governments step in or

not? If not, would that result to a cyber warfare that might have unknown implications to states and their public diplomacy?

Finally, there is the obvious concern about the public perception of such an act, as it could be understood as a weakness of the state to exercise its monopoly on the use of force. Laws that regulate the Internet and its use are national due to a lack of international agreements, but the question remains whether vigilante justice is the true path to justice or whether this leads even deeper into the Wild West analogy. However, it is difficult to imagine that companies operating in this legal grey area will be legally prosecuted, while on the other hand cyber criminals cannot be convicted. It is far more likely that authorities could eventually turn a blind eye to the active defense of companies, even if they appear to be crossing the line [62]. Whether it is tolerated or legalized, there are already many hack back activities underway by companies trying to defend their intellectual properties and critical assets from cyber espionage and sometimes seeking to thwart the aggressor forever. Nobody considers this to be lawful, but no one will be prosecuted for doing it [62].

5.3. Partners—A Possibility and a Cyber Threat Blind Spot

Partner CTAs were highly underreported, with 7 out of 22 organizations identifying them as a source of possible problems. At the same time partners have the trust to be accepted in restricted systems and places. There have been documented cases of supply-chain attacks [26]. In industrial environments the vendors are often responsible for the correct operation of their equipment. They can have backdoors into otherwise secure systems with the understanding that it is required for quick recovery in case of a malfunction.

FoF environments with additional levels of collaboration give the partners CTAs additional possibilities to cause harm. They have access to resources that will require mature security management processes and collaboration management tools to be both useful and secure. Finding the balance between access and security will be challenging.

Not only will the actions of the partners be interesting in a FoF environment, but also their current security status. As the trusted connections between partners enable circumventing cyber defenses, an active cyber incident detected at one partner's network can propagate to all partners.

It is important to keep in mind that the partners have de facto insider access to many resources in FoF systems and ignoring the risk of abuse is unacceptable. It is much harder to adapt to any security challenges by partners when compared to insiders. As insiders are typically employees of the organization, adapting their requirements to access or access rights to the FoF environment in a changing situation is easy. When dealing with partners it is much slower and more expensive to make any changes that are required. The changes may require changes to the legal agreement, requiring multiple rounds of lawyer overview for even small changes. This makes changes in the environment challenging if the required responses are not authorized and included in the partnership agreement. This makes partners a much more challenging CTA than insiders.

6. Conclusions

This paper analyzed CTAs listed by 22 different cyber security expert organizations. As expected, nation-state actors and cyber criminals were the most widely identified threat actors. Subsequently, more than half of the organizations listed terrorists (12), followed by insiders (11) and hacktivists (9) as the most frequently identified threat actors. Although terrorists are listed as an active threat actor by the majority of the assessed reports, high-profile incident involving cyber terrorist are unknown to the general public. The situation is quite different with the listing of industrial espionage. These threat actors are rather underrepresented in the reports, although there are repeatedly allegations that are published but not always proved.

The paper further grouped the 13 different CTAs that were identified by the expert organizations into 8 main CTA categories. This was done by analyzing the most probably motivation of each CTA and combining actors with similar types of motivation (e.g., ideology).

Since factory of the future (FoF) environments have special needs in terms of cyber security, this paper identified the main aspects of FoF environments that present cyber security challenges and

analyzed how the identified CTAs are likely to abuse them. This provides cyber security specialists working in a FoF environment a shortlist of the most likely CTAs targeting their environment. However, while the advanced FoF environment promises great benefits, the incremental challenges of cyber security that inherent connectivity presents must be properly addressed.

One of the CTAs with low identification ratings was that of competitors. Commercial competitors who run offensive cyber operations can have great benefits with low risks of blowback, at least in theory. There are, however, very few documented incidents related to such activities. The authors compared whether the behavior of corporate actors in other areas (e.g., legislation, patents, conventional industrial espionage) corresponded to the lack of cases in offensive cyber operations against competing corporations. There seems to be a mismatch with seemingly low number of cases of unethical corporate competition strategies in the cyber security area and the high number of cases in other areas.

While flexibility, efficiency and cost-effectiveness are considered as one of the driving factors for a successful FoF deployment, it is important to ensure that this environment is equipped with sophisticated and robust cyber security. Further research and technical development is needed to ensure that FoF systems are as cyber secure as the systems they are replacing. At the same time, competitors, who often operate on the edge of legality and sometimes beyond, must be perceived as a source of risk to take appropriate measures. This also applies to research that has so far missed addressing cyber threat actors in industrial espionage driven by competitors. Further research and an open debate is needed.

Author Contributions: MS contributed to almost all aspects of the paper., O-ML supported in most areas, with special focus on visualization; AS special focus in deepening the analysis of the competitor activity and hack back techniques; Conceptualization, MS. and O-ML; methodology, MS; investigation, MS, O-ML and AS; writing—original draft preparation, MS, O-ML and AS; writing—review and editing, MS, O-ML and AS; visualization, O-ML; All authors have read and agreed to the published version of the manuscript.

Funding: "This research was funded by ITEA3 Cyber Factory#1 project, grant number XXX"

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Chapple, M.; Stewart, J.M.; Rouse, M.; Gibson, D. Chapter 2 Personnel Security and Risk Management Concepts. In *Certified Information Systems Security Professional Official Study Guide*, 8th ed.; John Wiley & Sons: Hoboken, NJ, USA, 2018; p. 65.
2. National Institute of Standards and Technology—NIST. Guide to Industrial Control Systems (ICS) Security. May 2015. Available online: https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final (accessed on 23 April 2020).
3. Cyber Threat Source Descriptions. Available online: https://www.us-cert.gov/ics/content/cyber-threat-source-descriptions (accessed on 23 April 2020).
4. National Institute of Standards and Technology—NIST. Guide for Conducting Risk Assessments. September 2012. Available online: https://www.nist.gov/publications/guide-conducting-risk-assessments (accessed on 1 June 2020).
5. ENISA Threat Landscape Report 2018. Available online: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018 (accessed on 1 April 2020).
6. Canadian Centre for Cyber Security. Cyber Threat and Cyber Threat Actors. Available online: https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors (accessed on 30 April 2020).
7. Cybersecurity Strategy, National Center of Incident Readiness and Strategy for Cybersecurity. Available online: https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf (accessed on 15 April 2020).
8. A Report on Developments in the Field of Information and Telecommunications in the Context of International Security. Available online: https://undocs.org/A/74/120 (accessed on 11 November 2019).
9. Chinese National Internet Information Office. National Cyberspace Security Strategy. Available online: https://bit.ly/3cYCflV (accessed on 30 April 2020).

10. United States Information Technology Office. China Publishes National Security Strategy. Available online: http://www.usito.org/news/china-publishes-first-national-cybersecurity-strategy (accessed on 30 April 2020).
11. Doctrine of Information Security of the Russian Federation. Available online: http://www.scrf.gov.ru/security/information/DIB_engl/ (accessed on 22 February 2020).
12. A Strategy for Cybersecurity Governance in Brazil. Available online: https://igarape.org.br/wp-content/uploads/2019/01/A-Strategy-for-Cybersecurity-Governance-in-Brazil.pdf (accessed on 22 February 2020).
13. National Cybersecurity Policy Framework of South Africa. Available online: https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf (accessed on 22 February 2020).
14. National Cyber Security Strategy 2020 (NCSS 2020). Available online: https://ncss2020.nic.in/ (accessed on 23 April 2020).
15. Irwin, S. Creating a Threat Profile for Your Organization. Available online: https://www.sans.org/reading-room/whitepapers/threats/creating-threat-profile-organization-35492 (accessed on 22 March 2020).
16. International Securities Services Association. Cyber Security Risk Management in Securities Services. October 2018. Available online: https://www.issanet.org/e/pdf/2018-10_ISSA_Cyber_Risk_in_Securities_Services.pdf (accessed on 22 February 2020).
17. Global Cybersecurity Index 2018. ISBN 978-92-61-28191-5. Available online: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf (accessed on 23 April 2020).
18. Centre for Internet Security. Cybersecurity Spotlight—Cyber Threat Actors. Available online: https://www.cisecurity.org/spotlight/cybersecurity-spotlight-cyber-threat-actors/ (accessed on 13 January 2020).
19. International Common Criteria Conference. Common Criteria for Information Technology Security Evaluation. April 2017. Available online: https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf (accessed on 22 February 2020).
20. Verizon. 2019 Data Breach Investigations Report. Available online: https://enterprise.verizon.com/resources/reports/dbir/ (accessed on 22 February 2020).
21. IBM X-Force Threat Intelligence Index, 2020. Available online: https://www.ibm.com/security/data-breach/threat-intelligence (accessed on 22 February 2020).
22. 2020 Crowdstrike Global Threat Report. Crowdstrike Annual Publication. Available online: https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreat Report.pdf (accessed on 2 April 2020).
23. Cloud Security Threat Report (CSTR). June 2019, Volume 1. Available online: https://docs.broadcom.com/docs/cstr-1-en (accessed on 23 April 2020).
24. M-Trends 2020 Fireeye Mandiant Services|Special Report. Available online: https://content.fireeye.com/m-trends/rpt-m-trends-2020 (accessed on 13 February 2020).
25. Fortinet Threat Landscape Report Q3/19. Available online: https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-q3-2019.pdf (accessed on 23 April 2020).
26. Fortinet Threat Landscape Report Q4/18. Available online: https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-q4-2018.pdf (accessed on 23 April 2020).
27. McAfee Threats Report Q1/2019. Available online: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-aug-2019.pdf (accessed on 29 February 2020).
28. Cyber Threatscape Report. Available online: https://www.accenture.com/_acnmedia/pdf-107/accenture-security-cyber.pdf (accessed on 16 December 2019).
29. Anderson, R.; Barton, C.; Boehme, R.; Clayton, R.; Ganan, C.; Grasso, T.; Levi, M.; Moore, T.; Vasek, M. Measuring the Changing Cost of Cybercrime. WEIS 2019. Available online: https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_25.pdf (accessed on 15 April 2020).
30. Pratley, P. State-Sponsored Cyber Attacks. Available online: https://www.f-secure.com/en/consulting/our-thinking/state-sponsored-cyber-attacks (accessed on 25 March 2020).

31. Schwartz, M. Cybercrime-as-a-Service Economy: Stronger Than Ever. Available online: https://www.bankinfosecurity.com/cybercrime-as-a-service-economy-stronger-than-ever-a-9396 (accessed on 25 March 2020).
32. Finkle, J. Factbox: Cyber Warfare Expert's Timeline for Iran Attack. Reuters, December 2011. Available online: https://www.reuters.com/article/us-cyberattack-iran-idUSTRE7B10AV20111202 (accessed on 13 February 2020).
33. Buchanan, B. How North Korean Hackers Rob Banks Around the World. February 2020. Available online: https://www.wired.com/story/how-north-korea-robs-banks-around-world/ (accessed on 13 March 2020).
34. Bagge, D. *Unmasking Maskirovka: Russia's Cyber Influence Operations*; Defense Press New York, USA, 12 February 2019.
35. Schmitt, M. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*; Cambridge University Press: Cambridge, UK, 2017.
36. Mueller, R. *Report on the Investigation into Russian Interference in the 2016 Presidential Election*; U.S. Department of Justice: Washington, DC, USA, March 2019; p. 42. Available online: https://www.justice.gov/storage/report.pdf (accessed on 31 March 2020).
37. Kenney, M. Cyber-Terrorism in a Post-Stuxnet World. December 2015. Available online: https://www.researchgate.net/publication/270914520_Cyber-Terrorism_in_a_Post-Stuxnet_World (accessed on 12 January 2020).
38. Hackmageddon.com. Cyber Attack Timeline, Master Table. Available online: https://www.hackmageddon.com/2018-master-table/ (accessed on 15 December 2019).
39. Goodin, D. Here's the Netflix Account Compromise Bugcrowd doesn't Want You to Know About. 2020. Available online: https://arstechnica.com/information-technology/2020/03/bugcrowd-tries-to-muzzle-hacker-who-found-netflix-account-compromise-weakness/ (accessed on 25 March 2020).
40. Lyons, K. Zoom Vulnerability Would Have Allowed Hackers to Eavesdrop on Calls. Available online: https://www.theverge.com/2020/1/28/21082331/zoom-vulnerability-hacker-eavesdrop-security-google-hangouts-skype-checkpoint (accessed on 22 April 2020).
41. Cohen, F.B. Protection and Security on the Information Superhighway. Available online: http://all.net/books/superhighway/SuperHW.pdf (accessed on 9 March 2020).
42. Markoff, J. Oracle Leader Calls Microsoft Spying ,Civic Duty. Available online: https://www.nytimes.com/2000/06/29/business/oracle-leader-calls-microsoft-spying-civic-duty.html (accessed on 5 March 2020).
43. Dunn, P. Deliotte and the Ethics of Corporate Espionage. *Proc. Int. Assoc. Bus. Soc.* **2018**, *29*, 65–70.
44. Javers, E. Accountants and Spies: The Secret History of Deloitte's Espionage Practice. Available online: https://www.cnbc.com/2016/12/19/accountants-and-spies-the-secret-history-of-deloittes-espionage-practice.html (accessed on 3 March 2020).
45. Porter, M.E. *Competitive Strategy: Techniques for Analyzing Industries and Competitors*; University of Michigan Free Press: Ann Arbor, MI, USA, 1980.
46. Cf. Investopedia. Available online: https://www.investopedia.com/terms/g/gametheory.asp (accessed on 30 April 2020).
47. Grant, K. The Brand Protection Blog. April 2015. Available online: https://www.thebrandprotectionblog.com/cybersquatting-and-political-campaigns-no-laughing-matter/ (accessed on 3 January 2020).
48. Nowak, M.; Sigmund, K.A. A Strategy of Win-Stay, Lose-Shift that Outperforms Tit-for-Tat in the Prisoner's Dilemma Game. *Nature* **1993**, *364*, 56–58.
49. Bendor, J.; Diermeier, D.; Siegel, D.A.; Ting, M.M.A. *Behavioral Theory of Elections*; Princeton University Press: Princeton, NJ, USA, 2011.
50. Benitez, G.B.; Lima, R.F.; Frank, A.G.; Lerman, L.V. Understanding Industry 4.0: Definitions and insights from a cognitive map analysis. *Braz. J. Oper. Prod. Manag*. **2019**, *16*, 192–200, doi:10.14488/BJOPM.2019.v16.n2.a3.
51. World Economic Forum. White Paper Fourth Industrial Revolution Beacons of Technology and Innovation in Manufacturing. Available online: http://www3.weforum.org/docs/WEF_4IR_Beacons_of_Technology_and_Innovation_in_Manufacturing_report_2019.pdf (accessed on 30 April 2020).

52. Malatras, A.; Skouloudi, C.; Koukounas, A. Industry 4.0 Cybersecurity: Challenges & Recommendations. Available online: https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations (accessed on 12 January 2020).
53. McCabe, D.; Hong, N.; Benner, K. U.S. Charges Huawei with racketerring, adding pressure on China. Available online: https://www.nytimes.com/2020/02/13/technology/huawei-racketeering-wire-fraud.html (accessed on 9 March 2020).
54. Unites States Department of Justice. Unites States District Court Eastern District of New York against Huawei Technologies. Case 1:18-cr-00457-AMD, Doc. 126, Filed 02/13/20. Available online: https://www.justice.gov/opa/press-release/file/1248961/download (accessed on 9 March 2020).
55. Magen, S. Cybersecurity and Economic Espionage: The Case of Chinese Investments in the Middle East. In Cyber, Intelligence and Security. Available online: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/INSS-Cyber,%20Intelligence,%20and%20Security,%20Volume%201,%20No.%203.pdf (accessed on 19 March 2020).
56. Stanley, M.E. From China with Love: Espionage in the Age of Foreign Investment. *Brooklyn J. Int. Law* **2015**, *40*, 1033–1079.
57. Raice, S.; Dowell, A. Huawei Drpos U.S. Deal Amid Opposition. Available online: https://www.wsj.com/articles/SB10001424052748703407304576154121951088478 (accessed on 18 March 2020).
58. Barfield, C. Telecoms and the Huawei Conundrum—Chinese Foreign Direct Investment in the Unites States. In American Enterprise Institute. Available online: https://www.aei.org/wp-content/uploads/2011/11/-telecoms-and-the-huawei-conundrum-chinese-foreign-direct-investment-in-the-united-states_103528582558.pdf (accessed on 16 March 2020).
59. Crane, A. In the Company of Spies: When Competitive Intelligence Gathering becomes Industrial Espionage. *Bus. Horiz.* **2005**, *48*, 233–240.
60. Lindsay, N. Return of the "Hack Back" Active Cyber Defense Bill has Cybersecurity Experts Worried. Available online: https://www.cpomagazine.com/cyber-security/return-of-the-hack-back-active-cyber-defense-bill-has-cybersecurity-experts-worried/ (accessed on 3 March 2020).
61. Schmidle, N. The Digital Vigilantes Who Hack Back. Annals of Technology May 7, 2018 Issue. The New Yorker. Available online: https://www.newyorker.com/magazine/2018/05/07/the-digital-vigilantes-who-hack-back (accessed on 15 April 2020).
62. Kuchler, H. Cyber insecurity: Hacking Back. Financial Times. Available online: https://www.ft.com/content/c75a0196-2ed6-11e5-8873-775ba7c2ea3d (accessed on 15 April 2020).